12 May 1978

NOTE FOR: Mr. Robert W. Gambino
Chairman, DCI Security Committee

STAT FROM: [redacted]
Executive Secretary, DCI Security Committee

SUBJECT: E.O. 11652

1. Here is the latest copy of the replacement E.O. 11652. The President is expected to sign it on 24 May 1978. Anticipated effective date is 1 December 1978.

2. Our fix on NSA request for exemption to declassification procedures including exemption to review material subject to compartmentation under international agreement is adequate.

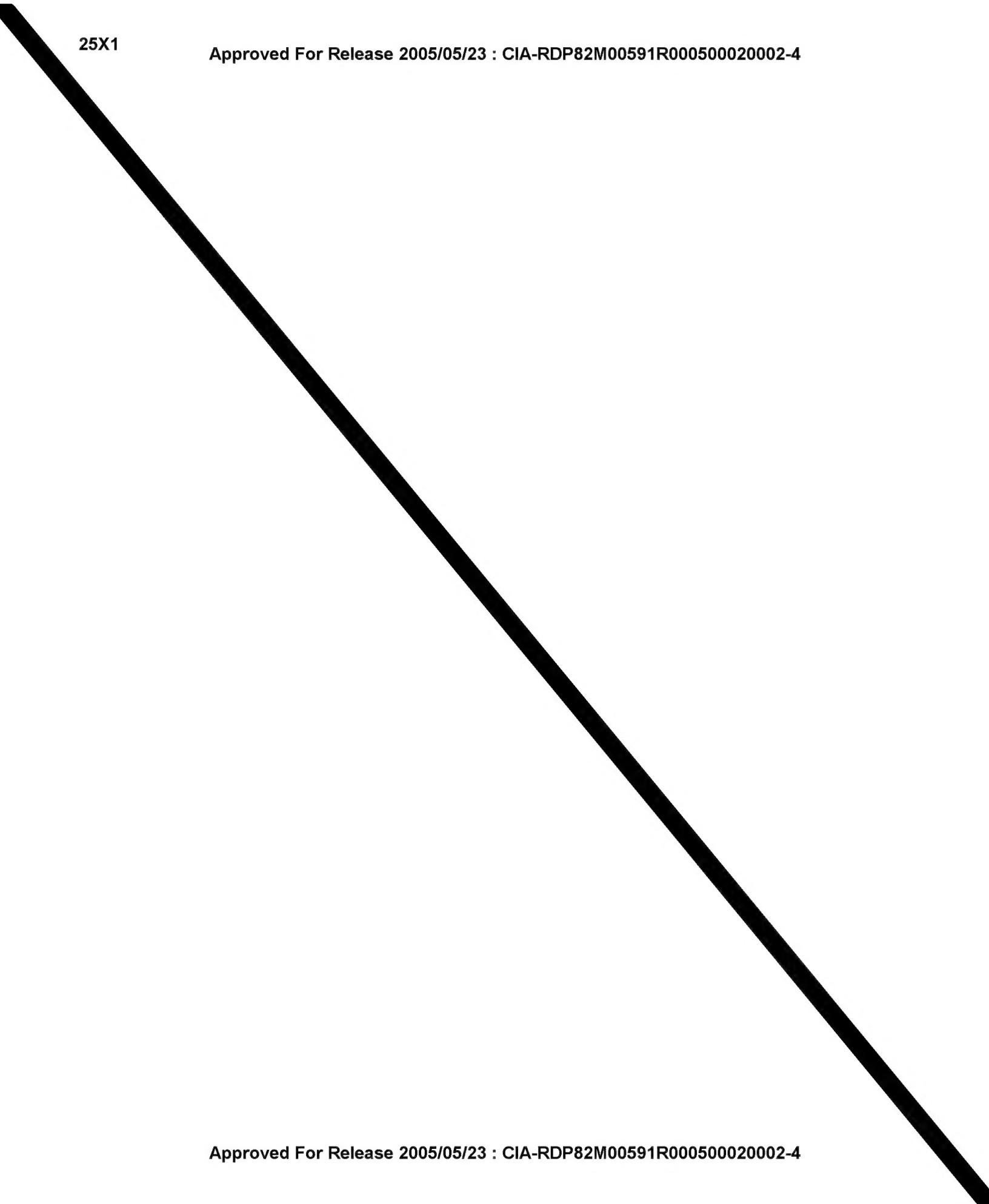
3. There is nothing here that would support NSA's suggestions to hold off on some of our NFIB action items.

4. The drafting of implementing actions is going well according
STAT to [redacted] sources. There is some observation by those doing the drafting that the lawyers lack the professional substantive knowledge necessary. Since fundamental security issues are involved, you should, at any chance you get, support a position which holds that substantive experts are required now and that lawyers should be relegated to an advisory role.

5. This would be a natural assignment for the Community Security Staff, but since we are not yet legal you might consider suggesting to Mr. Blake a willingness to appoint someone to this role from the Office of Security.

6. Unless we hear otherwise by 1630 hours on 12 May, I will inform
STAT [redacted] that SECOM has no objections. Nitpicking may come later, but for now, I think the Community has to live with this.

[redacted] STAT



Approved For Release 2005/05/23 : CIA-RDP82M00591R000500020002-4

DRAFT

May 3, 1978

EXECUTIVE ORDER

NATIONAL SECURITY INFORMATION

By virtue of the authority vested in me by the Constitution and laws of the United States of America; in order to balance the public's interest in access to government information with the need to protect certain national security information from disclosure, it is hereby ordered as follows:

TABLE OF CONTENTS

Section 1. Definitions.

(a) "Agency" has the meaning defined in 5 U.S.C. 552(e).

(b) "Classified information" means information or material (hereinafter collectively termed "information") that is owned by, produced for or by, or under the control of the United States Government; and that has been determined pursuant to this Order to require protection against unauthorized disclosure; and is so designated.

(c) "Foreign government information" means information that has been provided to the United States in confidence by, or produced by the United States pursuant to a joint arrangement requiring confidentiality with, a foreign government or international organization of governments or an official of either.

(d) "National security" means the national defense and foreign relations of the United States.

(e) "Declassification event" means an event, the occurrence of which would eliminate the need for continued classification.

Section 2. Original Classification.

(a) Classification Designation. Except as provided in the Atomic Energy Act of 1954 as amended, this Order provides the only basis for classifying information. Information may be classified in one of the three designations listed below. If there is reasonable doubt as to which designation is appropriate, or whether the information should be classified at all, the less restrictive treatment should

be designated.

(1) "Top Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) "Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security.

(b) Classification Authority.

(1) Top Secret. Authority for original classification of information as "Top Secret" may be exercised only by the President, by such officials as the President may designate by publication in the Federal Register, by the Agency heads listed below, and by officials to whom such authority is delegated in accordance with the provisions of subsection (4) below:

The Secretary of State

The Secretary of the Treasury

The Secretary of Defense

The Secretary of the Army

The Secretary of the Navy

The Secretary of the Air Force

The Attorney General of the United States

The Secretary of Energy

The Chairman, Nuclear Regulatory Commission

The Director, Arms Control and Disarmament Agency

The Director of Central Intelligence

The Administrator, National Aeronautics and Space Administration

The Administrator, General Services Administration (delegable only to the Director, Federal Preparedness Agency and to the Director, Information Security Oversight Office.)

(2) Secret. Authority for original classification of information as "Secret" may be exercised only by such officials as the President may designate by publication in the Federal Register, by the Agency heads listed below, by officials who have "Top Secret" classification authority and by officials to whom such authority is delegated in accordance with the provisions of subsection (4):

The Secretary of Transportation

The Administrator, Agency for International Development

The Director, International Communications Agency

(3) Confidential. Authority for original classification of information as "Confidential" may be exercised only by such officials as the President may designate by publication in the Federal Register, by the agency heads listed below, by officials who have "Top Secret" or "Secret" classification authority and by officials to whom such authority is delegated in accordance with subsection (4):

The President and Chairman, Export-Import Bank of the United States

The President and Chief Executive Officer, Overseas Private Investment Corporation

(4) Limitations on Delegation of Classification Authority.

(i) Authority for original classification of information as "Top Secret" may be delegated only to principal subordinate officials determined by the President or by Agency heads listed in subsection (1) above to have a frequent need to exercise such authority.

(ii) Authority for original classification of information as "Secret" may be delegated only to subordinate officials determined by the President, by agency heads listed in subsections (1) and (2) above and by officials with "Top Secret" classification authority to have frequent need to exercise such authority.

(iii) Authority for original classification of information as "Confidential" may be delegated only to subordinate officials determined by the President, by agency heads listed in subsections (1), (2) and (3) above, and by officials with "Top Secret" classification authority to have frequent need to exercise such authority.

(iv) Delegated original classification authority may not be redelegated.

(v) Each delegation of original classification authority shall be in writing.

(vi) Delegations of original classification authority shall be held to an absolute minimum. Administrative convenience is not a valid basis for such delegations. Periodic review of such delegations shall be made to ensure that the officials so designated have demonstrated a continuing need to exercise such authority.

(5) Exceptional Cases. When an employee or contractor of an agency that does not have original classification authority originates information believed to require classification, the information shall be protected in the manner prescribed by this Order and implementing directives. The information shall be transmitted promptly under appropriate safeguards to the agency which has appropriate subject matter interest and classification authority. That agency shall decide within 30 days whether to classify the information. If it is not clear which agency should get the information, it shall be sent to the Director of the Information Security Oversight Office established in Section 6 for a determination.

(c) Classification Requirements.

(1) Information may not be classified unless an original classification authority determines both: (1) that the information falls into one or more of the criteria set forth in subsection (3) below; and (2) that unauthorized disclosure of the information reasonably could be expected to cause at least identifiable damage to the national security.

(2) Unauthorized disclosure of foreign government information or the identity of a confidential foreign source is presumed to cause at least identifiable damage to the national security.

(3) Information may not be considered for classification unless it concerns:

(i) military plans, weapons, or operations; or

(ii) foreign government information; or

(iii) intelligence sources or methods; or

(iv) foreign relations or foreign activities of the United States; or

(v) scientific, technological, or economic matters relating to the national security; or

(vi) other matters determined by the President, a person designated by the President pursuant to Sec. 2(b)(1) or an agency head to be related to national security and to require protection

against unauthorized disclosure.

(4) Each determination under criterion (vi) above shall be reported when it is made to the Director of the Information Security Oversight Office.

(d) Limitation on Duration of Classification.

(1) Except as permitted in paragraph (2) below, at the time of original classification each original classification authority shall set a date or event for automatic declassification no more than six years later.

(2) Only officials with Top Secret classification authority and agency heads listed in Section 2(b) may classify information for more than six years from the date of original classification. This authority shall be used sparingly. In such cases, a declassification date or event or a date for review shall be set as early as national security permits. This date or event shall be no more than twenty years after original classification, except that for foreign government information the date or event may be up to thirty years after original classification.

(e) Classification Identification and Marking.

(1) At the time of origination, the following shall be shown on the face of paper copies of all classified documents: (i) the identity of the original classification authority; (ii) the office of origin; (iii) the date of the document's classification; (iv) the date or event for declassification or review; and (v) one of the three classification designations defined above. Documents classified for more than six years also shall be marked with the identity of the official who authorized the prolonged classification and the reason classification is expected to remain necessary despite the passage of time. These markings may be by reference to criteria set forth in agency implementing regulations. When the individual who signs or otherwise authenticates a document also is authorized to classify it, no further annotation of identity is required.

(2) Only the designations presribed by this Order may be used to identify classified information. Markings such as "For Official Use Only" and "Limited Official Use" may not be used for that purpose. Terms such as "Conference," or "Agency" may not be used in conjunction with the classification designations prescribed by this Order; e.g., "Agency Confidential," or "Conference Confidential."

(3) In order to facilitate excerpting and other uses, each classified document shall, by marking or other means, indicate clearly which portions are classified, with the applicable classification designation, and which portions are not classified. The Director of the Information Security Oversight Office may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information.

(4) Foreign government information either shall retain its original classification designation or be assigned a United States classification designation that shall assure a degree of protection equivalent to that required by the entity that furnished the information.

(5) Classified documents that contain or reveal information that is subject to special dissemination and reproduction limitations authorized under this Order shall be marked clearly so as to place the user on notice of the restrictions.

(f) Prohibitions.

(1) Classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.

(2) Basic scientific research information not clearly related to the national security may not be classified.

(3) A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified under this Order until and unless the government acquires a proprietary interest in the product. This Order does not affect the provisions of the Patent Secrecy Act of 1952 (45 U.S.C. 181-188).

(4) References to classified documents that do not disclose classified information may not be classified or used as a basis for classification.

(5) Classification may not be used to limit dissemination of information that is not classifiable under the provisions of this Order, or to prevent or delay the public release of such information.

(6) No document originated on or after the effective date of this Order may be classified after an agency has received a request for the document under the Freedom of Information Act or the Mandatory Review provision of this Order (Section 4(f)), unless such classification

is consistent with this Order and is authorized by the agency head. Documents originated before the effective date of this Order and subject to such a request also may be classified under this Order by the senior official designated to oversee the agency information security program and by officials with Top Secret classification authority. Classification authority under this paragraph shall be exercised personally, on a document-by-document basis.

(7) Classification may not be restored to documents already declassified and released to the public under this Order or prior Orders.

Section 3. Derivative Classification of Information.

(a) Original classification authority shall not be given to persons who only reproduce, extract or summarize classified information or who only apply classification markings derived from source material or as directed by a classification guide. Persons who apply such derivative classification markings shall (1) respect classifications assigned by originators; (2) verify the information's current level of classification so far as practicable before applying the markings; (3) carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings, in accordance with subsections (b) and (c) below. A single marking may be used for documents based on multiple sources.

(b) Classification guides used to direct derivative classification shall specifically identify the information to be classified. A decision to identify information for protection in this manner constitutes an original classification decision. Each classification guide shall specifically indicate how the designations, time limits, markings, and other requirements of this Order are to be applied to the information. Each such guide shall be approved personally and in writing, by an agency head listed in Section 2(b) or by an official with Top Secret classification authority.

(c) New material that derives its classification from information classified on or after the effective date of this Order shall be marked with the declassification date or event or the date for review assigned to the source information.

(d) New material that derives its classification from information classified under prior Orders shall be treated as follows:

(1) If the source material bears a declassification date or event twenty years or less from the date of origin, that date or event shall be carried forward on the new material.

(2) If the source material bears no declassification date or event or is marked for declassification beyond twenty years, the new material shall be marked with a date for review for declassification at twenty years from the date of original classification of the source material.

(3) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond thirty years, the new material shall be marked for review for declassification at thirty years from the date of original classification of the source material.

Section 4. Declassification and Downgrading

(a) Declassification Authority. The authority to declassify or downgrade information classified under this or prior Executive orders shall be exercised as follows:

(1) Classified information may be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position, by a successor, or by a supervisory official of either.

(2) Agency heads named in Section 2(b) shall designate additional officials at the lowest practicable echelons to exercise declassification and downgrading authority.

(3) When the Director of the Information Security Oversight Office determines that information is classified in violation of this Order the Director may require the information to be declassified by the agency that originated the declassification. Any decision by the Director may be appealed to the National Security Council. The information shall remain classified until the appeal is decided or until one year from the date of the appeal, whichever occurs first. The same procedure shall be followed when the Director declassifies information pursuant to the appellate function in Section 4(f)(2).

(4) The provisions of this Order relating to declassification shall also apply to agencies which, under the terms of this Order, do not have original classification authority but which had such authority under prior

Orders.

(b) Authority Over Transferred Information.

(1) For classified information transferred in conjunction with a transfer of function -- not merely for storage purposes -- the receiving Agency shall be deemed to be the originating Agency for all purposes under this Order.

(2) For classified information not transferred in accordance with subsection (1) above, but originated in an Agency which has ceased to exist, each Agency in possession shall be deemed to be the originating Agency for all purposes under this Order. Such information may be declassified or downgraded by the Agency in possession after consulting with any other Agency having an interest in the subject matter.

(3) Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and Agency guidelines.

(4) After the termination of a Presidential administration, the Archivist of the United States may review and declassify or downgrade all information classified by the President, the White House staff, committees or commissions appointed by the President or others acting on the President's behalf. This authority shall be exercised only after consultation with the agencies having primary subject matter interest. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office

(c) Declassification Policy.

(1) Declassification of classified information shall be given emphasis comparable to that accorded classification. Information classified pursuant to this and prior Orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or the occurrence of an event which would make continued classification unnecessary.

(2) Whenever information is reviewed for declassification, it shall be declassified unless the declassification authority established in Section 4(a) determines that the information continues to meet the standards for classification prescribed in Section 2(c) despite the passage of time.

(3) It is presumed that information which continues to meet the standards for classification in Section 2(c) requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head; or the senior agency officials with responsibility for processing Freedom of Information Act requests and Mandatory Review requests under this Order; or officials with Top Secret classification authority; or the Archivist of the United States in the case of material covered in Section 4(f)(2). That official will determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

NO PAGES
13 or 14
IN THIS DRAFT
(SHORTENED)

(e) Systematic Review for Declassificaton.

(1) Classified information constituting permanently valuable records of the Government as defined by 44 U.S.C. 2103 and information in the possession and control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107 note shall be reviewed for declassification as it becomes 20 years old. Agency heads listed in Section 2(b) and officials designated by the President pursuant to Section 2(b)(1) of this Order may extend classification beyond 20 years, but only in accordance with Sections 4(c) and 4(e)(2). This authority may not be delegated. When classification is extended beyond 20 years, a date for declassification or the next review no more than 10 years later shall be set and marked on the document. Subsequent reviews for declassification shall be set at no more than 10 year intervals. The Director of the Information Security Oversight Office may extend the period between subsequent reviews for specific categories of documents or information.

(2) Within 180 days after the effective date of this Order, the agency heads listed in Section 2(b) and the heads of agencies which had original classification authority under prior orders shall, after consultation with the Archivist of the United States and review by the Information Security Oversight Office, issue and maintain guidelines for systematic review covering 20-year old classified information under their jurisdiction. These guidelines shall state specific, limited categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond 20 years is needed. These guidelines shall be authorized for use by may, upon approval of the issuing authority, be used the Archivist of the United States and by any Agency having custody of the information. All information not identified in these guidelines as requiring review and for which a prior automatic declassification date has not been established shall be declassified automatically at the end of 20 years from the date of original classification.

(3) Notwithstanding Section 4(e)(1) and (2), the Secretary of Defense may establish special procedures for systematic review and declassification of classified cryptologic information produced by units of the Department of Defense. These procedures shall be consistent, so far as practicable, with the objectives of Section 4 (e) (1) and (2). They shall be approved by the Director of the Information Security Oversight Office and, with respect to matters pertaining to intelligence sources and methods, shall be reviewed by the Director of Central Intelligence prior to implementation. Any decision by the Director of the Information Security Oversight Office may be appealed to the National Security Council. The information shall remain classified until the appeal is decided or until one year from the date of the appeal, whichever occurs first.

(4) Foreign government information shall be exempt from automatic declassification and 20 year systematic review. Unless declassified earlier, such information shall be reviewed for declassification 30 years from its date of origin. Such review shall be in accordance with the provisions of Section 4(c) and with guidelines developed by agency heads in consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned.

(5) Transition to systematic review at twenty years shall be implemented as rapidly as practicable and shall be completed no more than ten years from the effective date of this Order.

(f) Mandatory Review for Declassification.

(1) Except as provided in (2) below, information classified pursuant to this Order or prior Orders shall be reviewed for possible declassification upon request of a member of the public, a government employee or an agency, provided the request is sufficiently specific to permit location of the information with reasonable effort. Requests for declassification under this provision shall be acted upon within 60 days. Requests for declassification under the Freedom of Information Act shall be processed in accordance with the provisions of the Act.

(2) Information less than ten years old originated by the President, the White House staff, or committees or commissions appointed by the President or others acting on behalf of the President, including such information in the possession and control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107 note is exempted from the provisions of subsection (1) above. Such information over ten years old, however, shall be subject to mandatory review for declassification. The processing of such requests for mandatory review shall accord with procedures developed by the Archivist of the United States which shall include consultations with agencies having primary subject matter interest. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision and may follow the appeals process set forth in Section 4(a)(3).

(3) Requests for declassification of classified documents originated by an agency but in the possession and control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107 note shall be referred by the Archivist to the Agency of origin for processing in accordance with subsection (1) above and for direct response to the requestor. The Archivist shall inform requestors of such referrals.

(4) No agency in possession of a classified document may, in response to a request for the document made under the Freedom of Information Act or this Order's Mandatory Review provision, refuse to confirm the existence or non-existence of the document, unless the fact of its existence or non-existence would itself be classifiable under this Order.

(g) Downgrading. Classified information that is marked for automatic downgrading is downgraded accordingly without notification to holders. Other classified information may be assigned a lower classification designation by the originator or by other authorized officials when such downgrading is appropriate. Notice of such downgrading shall be provided to holders of the information to the extent practicable.

Section 5. Safeguarding.

(a) General Restrictions on Access.

(1) No person may be given access to classified information unless that person has been determined to be trustworthy and unless access is necessary for the performance of official duties.

(2) All classified information shall be marked conspicuously to put users on notice of its current classification status and, if appropriate, to show any special distribution or reproduction restrictions authorized by this Order.

(3) Controls shall be established by each agency to assure that classified information is used, processed, stored, reproduced and transmitted only under conditions that will provide adequate protection and prevent access by unauthorized persons.

(4) Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of Chapters 21 and 33 of Title 44 of the United States Code governing disposition of federal records.

(5) Classified information disseminated outside the executive branch shall be given protection equivalent to that afforded within the executive branch.

(b) Special Access Programs.

(1) Agency heads listed in Section 2(b)(1) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or prior Orders. Such programs may be created or continued only by written direction and only by these agency heads and, for matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. Classified information in such programs shall be declassified according to the provisions of Section 4. Special access programs may be created or continued only on a specific showing that:

(i) normal management and safeguarding procedures are not sufficient to limit need-to-know or access;

(ii) the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved; and

(iii) the special access controls balance the need to protect the information against the full spectrum of needs to use the information.

(2) All such special access programs shall be reviewed regularly and, except those required by treaty or international agreement, shall terminate automatically every five years unless renewed in accordance with procedures in this subsection.

(3) Within 180 days after the effective date of this Order, agency heads shall review all existing special access programs under their jurisdiction and continue them only in accordance with the procedures in this subsection. Each of those Agency heads shall also establish and maintain a system of accounting for special access programs.

The Director of the Information Security Oversight Office shall have non-delegable access to all such accountings.

(c) Access by Historical Researchers and Former Presidential Appointees. The requirement in Section 5(a)(1) that access to classified information be granted only as is necessary for the performance of official duties may be waived with respect to persons who are engaged in the historical research projects or who previously have occupied policy-making positions to which they were appointed by the Presiden provided that the agency with jurisdiction over the information:

(1) makes a written determination that access is consistent with the interest of national security;

(2) takes appropriate steps to ensure that classified information is not disclosed or published without prior review and declassification;

(3) takes reasonable action to ensure that access is limited to specific categories of information over which that agency has classification jurisdiction;

(4) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed or received while serving as a Presidential appointee.

(d) Reproduction Controls.

(1) Top Secret documents may not be reproduced without the consent of the originating agency unless otherwise marked by the originating office.

(2) Reproduction of Secret and Confidential documents may be restricted by the originating agency.

(3) Reproduced copies of classified documents are subject to the same accountability and controls as the original documents.

(4) Records shall be maintained by all agencies that reproduce paper copies of classified documents to show the number and distribution of reproduced copies of all Top Secret documents; all documents covered by special access programs distributed outside the originating agency; and all Secret and Confidential documents marked in accordance with Section 2(b)(5).

(5) Subsections (1) and (2) above shall not restrict the reproduction of documents for the purpose of facilitating review for declassification. However, such reproduced documents that remain classified after review must be destroyed after they are used.

Section 6. Implementation and Review.

The National Security Council may review all matters with respect to the implementation of this Order and shall provide overall policy direction for the information security program.

(a) Information Security Oversight Office.

(1) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. This responsibility shall be delegated to an Information Security Oversight Office.

(2) This Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Administrator also shall have authority to appoint a staff for the Office.

(3) The Director shall:

(i) oversee agency actions to ensure compliance with this Order and implementing directives of the Information Security Oversight Office.

(ii) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program, including appeals from decisions on declassification requests pursuant to Section 4(f)(2);

(iii) exercise the authority to declassify information provided by Sections 4(a)(3) and 4(f)(2);

(iv) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order which shall be binding on the agencies;

(v) report annually to the President through the Administrator of General Services and the National Security Council on the implementation of this Order;

(vi) review all agency implementing regulations and guidelines. The Director may require any regulation or guideline that is not consistent with this Order or implementing directives to be changed. Any decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect until the appeal is decided or until one year from the date of the appeal, whichever occurs first.

(vii) exercise case-by-case classification authority in accordance with Section 2(b)(5) and review requests for original classification authority from agencies or officials not granted original classification authority under Section 2 of this Order;

(viii) have the authority to conduct on-site reviews of the information security program of each agency that handles classified information and to require of each agency such reports, information, and other cooperation as necessary to fulfill the above responsibilities. If such reports, inspection, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head may deny access. The Director may appeal denials to the National Security Council. The denial of acess shall remain in effect until the appeal is decided or until one year from the date of the appeal, whichever occurs first.

(b) Interagency Information Security Committee. There is established an Interagency Information Security Committee which shall be chaired by the Director and shall be comprised of representatives of the Secretaries of State, Defense, Treasury and Energy, the Attorney General, the Director of Central Intelligence, the National Security Council Staff, the Domestic Policy Staff, and the Archivist of the United States. Representatives of other agencies may be invited to meet with the Committee on matters of particular interest to those agencies. The Committee shall meet at the call of the Chairman or at the request of a member Agency and shall advise the Chairman on implementation of this Order.

(c) Agencies with Original Classification Authority. Each agency granted original classification authority pursuant to this Order shall:

(1) Submit to the Information Security Oversight Office a copy of all regulations and guidelines for systematic review adopted pursuant to this Order and implementing directives. Subsequent changes to Agency regulations and guidelines for systematic review shall also be forwarded to the Oversight Office.

(2) Develop, to the extent practicable, and publish in the Federal Register unclassified regulations implementing this Order.

(3) Designate an agency official to conduct an active oversight program to ensure effective implementation of this Order.

(4) Designate a senior agency official or chair an agency committee with authority to act on all suggestions and complaints with respect to the agency's administration of the information security program.

(5) Establish a process to decide appeals from denials of declassification requests, pursuant to Section 4(f).

(6) Establish a program to familiarize agency personnel and others with access to classified information with the provisions of this Order and implementing directives. This program shall impress upon agency personnel their responsibility to exercise vigilance in complying with this Order. The program shall encourage agency personnel to challenge through Mandatory Review and other appropriate procedures classification decisions believed to be improper.

(7) Ensure the preparation and promulgation of guidelines for security classification that will facilitate the identification and uniform classification of information requiring protection under the provisions of this Order.

(8) Develop and promulgate guidelines for systematic review in accordance with Section 4(e)(2).

(9) Take necessary action to ensure that:

(i) a demonstrable need for access to classified information is established prior to the initiation of administrative clearance procedures, and

(ii) the number of people granted access to classified information is reduced to and maintained at the minimum, consistent with operational requirements and needs.

(10) Ensure that safeguarding practices are reviewed continuously and eliminate those that are duplicative or unnecessary.

(11) Submit to the Information Security Oversight Office such information or reports as the Director of the Office may find necessary to carry out the Office's responsibilities.

(d) Agencies Without Original Classification Authority.

Each Agency that has not been granted original classification authority but that handles classified information shall comply with appropriate subsections above /(c)(1), (2), (3), (4), (5), (6), (8), (9), (10) and (11)_7.

Section 7. Administrative Sanctions.

In any case in which the Information Security Oversight Office finds that a violation of this Order or any implementing directive has occurred, it shall make a report to the head of the agency concerned so that corrective steps may be taken.

(a) Officers and employees of the United States shall be subject to appropriate administrative sanctions if they:

(1) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or

(2) knowingly, willfully and without authorization disclose information properly classified under this Order or prior Orders or compromise properly classified information through negligence; or

(3) knowingly and willfully violate any other provision of this Order or implementing directive.

(b) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and Agency regulations.

(c) Agency heads shall make provision to ensure that appropriate and prompt corrective action is taken whenever a violation under subsection (a) occurs. The Director of the Information Security Oversight Office shall be informed when such violations occur.

(d) Agency heads shall report to the Attorney General evidence of possible violations of federal criminal law by an employee of their department or agency to the extent any such information may be reflected in classified information and report to the Attorney General evidence of possible violations by any other person of those federal criminal laws specified in guidelines adopted by the Attorney General;

Section 8. Atomic Energy Information or Material.

Nothing in this Order shall supersede any requirements made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and information designated as "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of such Atomic Energy Act and the regulations of the Department of Energy.

Section 9. Interpretation of the Order.

The Attorney General, upon request by the head of an Agency, his duly designated representative, or the Director of the Information Security Oversight Office, shall personally or through authorized representatives of the Department of Justice render an interpretation of this Order with respect to any question arising in the course of its administration.

Section 10. Revocation of Prior Orders and Directives.

Executive Order No. 11652 of March 8, 1972, as amended by Executive Order No. 11714 of April 24, 1973, and No. 11862 of June 11, 1975, and the National Security Council Directive of May 17, 1972 [3 C.F.R. 1085 (1971-75 Comp.)] are revoked.

Section 11. Effective Date.

This Order shall become effective on December 1, 1978, except that the functions of the Information Security Oversight office specified in Section 6(a)(1)(iv) and 6(a)(1)(vi) shall be effective immediately and shall be performed in the interim by the Interagency Classification Review Committee established pursuant to Executive Order 11652.